国家工程研究中心和天枢智库联合出品

数字安全观察

DIGITAL SECURITY INSIGHT

数据安全专刊 No. 003(总第 135 期)

责编：钟力 zhongli1@360.cn

导　读

第三期《数字安全观察·数据安全专刊》重点回顾总结2022年第一季度的整体数据安全态势，分为政策形势，两会声音，技术、产品与市场趋势和勒索事件专题四个板块，主要内容如下：

政策形势方面，数字经济发展和数据要素价值成为2022年第一季度热点。在国家层面，国务院正式印发《“十四五”数字经济发展规划》（简称《规划》），这是我国数字经济领域的首部国家级专项规划，也是顺应数字经济时代需求的产物，为“十四五”时期推动数字经济健康发展提供了重要指引。地方层面，上海、贵州、广东等地纷纷颁布相关数据条例，积极响应国家不断做强做优做大我国数字经济号召。

两会声音方面，数据安全、个人信息保护、数据要素与数据确权、东数西算等关键词成为今年两会热点。2022年是数字安全元年，随着数字化转型的深入，数据安全挑战也越来越大，数据安全和个人信息保护成为发展的前提；同时，数字经济时代，数据作为一种资产，数据要素与数据确权也成为了关注热点；“东数西算”作为国家重要战略工程，在今年两会上成为代表委员热议的话题，“东数西算”可以充分发挥我国体制优势，优化全国算力基础设施分布，实现全国一体化布局。

技术、产品与市场洞察方面，数据安全产品和市场增长明显。技术方面，隐私计算发展引人注目，谷歌宣布推出Android隐私沙盒、

多方安全计算金融应用产品被重磅纳入国推认证；市场方面，有三大热点值得关注。一是未来五年全球企业数据泄露防护（DLP）市场预计将以21.03%的复合年增长率高速增长，到2026年市场规模将达到62.65亿美元。二是在安全服务市场发展中，据IDC预测，到2025年，咨询服务市场的规模将达到24.6亿美元。三是据Research And Markets数据显示，零信任安全市场将在2027年达到644亿美元。

勒索事件专题方面，在这几年勒索软件呈爆发式增长的背景下，2022年第一季度勒索攻击事件频发，受害者中不乏一些全球知名的企业和组织。在巨大的利润驱使下，许多网络犯罪分子前赴后继，勒索软件已经变成当前网络犯罪主要的商业模式，这也导致了企业数据泄露的规模和风险不断扩大，给全球经济发展和社会稳定带来了严重的影响。本部分针对第一季度较为活跃的勒索软件组织，如Lapsus$、Conti、LockBit，回顾勒索攻击事件经过，呈现其活动轨迹。

目 录

一、政策形势

2022 年第一季度的政策形势重点围绕数字经济、地方数据战略、条例等，国家数字经济发展开始逐步步入正轨。国家层面，《“十四五”数字经济发展规划》、《要素市场化配置综合改革试点总体方案》等国家指导文件正式发布，国家“东数西算”工程全面启动，我国数字经济正在迎来新一轮的变革。地方层面，各地加快布局数字经济，《上海市推进治理数字化转型实现高效能治理行动方案》、《贵州省大数据战略行动 2022 年工作要点》、《河南省数字经济促进条例》等政策文件纷纷出台，有力支撑数字经济健康发展，为地方数字经济发展提供引领带动作用。

（一）国家政策法规

1、《要素市场化配置综合改革试点总体方案》

1 月 6 日，国务院办公厅印发《要素市场化配置综合改革试点总体方案》，推动要素市场化配置改革向纵深发展。《方案》提出了八个方面试点任务，包括:进一步提高土地要素配置效率，推动劳动力要素合理畅通有序流动，推动资本要素服务实体经济发展，大力促进技术要素向现实生产力转化，**探索建立数据要素流通规则**，加强资源环境市场制度建设，健全要素市场治理，进一步发挥要素协同配置效应。

《方案》在“探索建立数据要素流通规则”方面中提出了四项任务:

一、完善公共数据开放共享机制。建立健全高效的公共数据共享协调机制。**二、建立健全数据流通交易规则。**探索“原始数据不出域、数据可用不可见”的交易范式。**三、拓展规范化数据开发利用场景。**发挥领军企业和行业组织作用，推动人工智能、区块链、车联网、物联网等领域数据采集标准化。**四、加强数据安全保护。**强化网络安全等级保护要求。

（来源：中国政府网）

2、《“十四五”数字经济发展规划》

1 月 12 日，国务院印发了“十四五”数字经济发展规划，是我国数字经济领域的首部国家级专项规划。《规划》明确了“十四五”时期推动数字经济健康发展的指导思想、基本原则、发展目标、重点任务和保障措施。

《规划》部署了八方面重点任务：一是优化升级数字基础设施。二是充分发挥数据要素作用。三是大力推进产业数字化转型。四是加快推动数字产业化。五是持续提升公共服务数字化水平。六是健全完善数字经济治理体系。强化协同治理和监管机制，增强政府数字化治理能力，完善多元共治新格局。七是着力强化数字经济安全体系。增强网络安全防护能力，提升数据安全保障水平，有效防范各类风险。八是有效拓展数字经济国际合作。围绕八大任务，《规划》明确了信息网络基础设施优化升级等十一个专项工程。

（来源：中国政府网）

3、《关于推动平台经济规范健康持续发展的若干意见》

1 月 19 日，国家发展改革委、市场监管总局、中央网信办、工业和信息化部、人力资源社会保障部、农业农村部、商务部、人民银行、税务总局等 9 部门发布《关于推动平台经济规范健康持续发展的若干意见》。

《意见》指出，修订《反垄断法》，完善数据安全法、个人信息保护法配套规则。同时指出，探索数据和算法安全监管。切实贯彻收集、使用个人信息的合法、正当、必要原则，严厉打击平台企业超范围收集个人信息、超权限调用个人信息等违法行为。从严管控非必要采集数据行为，依法依规打击黑市数据交易、大数据杀熟等数据滥用行为。在严格保护算法等商业秘密的前提下，支持第三方机构开展算法评估，引导平台企业提升算法透明度与可解释性，促进算法公平。严肃查处利用算法进行信息内容造假、传播负面有害信息和低俗劣质内容、流量劫持以及虚假注册账号等违法违规行为。推动平台企业深入落实网络安全等级保护制度，探索开展数据安全风险态势监测通报，建立应急处置机制。国家机关在执法活动中应依法调取、使用个人信息，保护数据安全。

（来源：国家发改委）

5、《网络安全审查办法》正式实施

2 月 15 日，国家互联网信息办公室、国家发展和改革委员会等十三部门联合发布的《网络安全审查办法》（以下简称《办法》）正式实施。《办法》对上市审查申报的要求、时机和主体都做了明确要求。《办法》第七条提出，掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须申报审查。中国网络安全审查技术与认证中心设立网络安全审查咨询窗口，开始接收网络平台运营者赴国外上市的审查申报。

（来源：中国网信网）

6、“东数西算”国家工程全面启动

2 月 17 日，国家发展改革委、中央网信办、工业和信息化部、国家能源局近日联合印发文件，同意在京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏启动建设国家算力枢纽节点，并规划了张家口集群等 10 个国家数据中心集群。至此，全国一体化大数据中心体系完成总体布局设计，“东数西算”工程正式全面启动。

按照全国一体化大数据中心体系布局，8 个国家算力枢纽节点将作为我国算力网络的骨干连接点，发展数据中心集群，开展数据中心与网络、云计算、大数据之间的协同建设，并作为国家“东数西算”工程的战略支点，推动算力资源有序向西转移，促进解决东西部算力供需失衡问题。

“东数西算”中的“数”，指的是数据，“算”指的是算力，即对数据的处理能力。“东数西算”是通过构建数据中心、云计算、大数据一体化的新型算力网络体系，将东部算力需求有序引导到西部，优化数据中心建设布局，促进东西部协同联动。

（来源：中国政府网）

7、国务院：加强电子证照应用安全管理，严格保护信息安全

国务院办公厅发布《关于加快推进电子证照扩大应用领域和全国互通互认的意见》。《意见》共五章十八条，包括总体要求、扩大电子证照应用领域、推动电子证照全国互通互认、全面提升电子证照应用支撑能力和保障措施。

其中强调加强电子证照应用安全管理和监管。加强电子证照签发、归集、存储、使用等各环节安全管理，严格落实网络安全等级保护制度等要求，强化密码应用安全性评估，探索运用区块链、新兴密码技术、隐私计算等手段提升电子证照安全防护、追踪溯源和精准授权等能力。按照信息采集最小化原则归集数据，对共享的电子证照进行分类分级管理，避免信息泄露。加快推进国家网络身份认证公共服务基础设施建设和应用，加强对电子证照持证主体、用证人员的身份认证、授权管理和个人信息保护。强化企业和群众身份认证支撑，增强电子证照签发和使用等环节的统一身份认证能力。建立健全严格的责任追究制度，依法严厉打击电子证照制作生成过程中的造假行为，杜绝未

经授权擅自调用、留存电子证照信息，切实保障电子证照及相关信息合法合规使用，保护持证主体的商业秘密和个人信息。

（来源：中国电子政务网）

8、《2022 年提升全民数字素养与技能工作要点》

中央网信办、教育部、工业和信息化部、人力资源社会保障部联合印发《2022 年提升全民数字素养与技能工作要点》（以下简称《工作要点》）。通知要求，要坚持以习近平新时代中国特色社会主义思想为指导，以满足人民日益增长的美好生活需要、促进人的全面发展和全体人民共同富裕为根本目的，坚持目标导向、问题导向、结果导向，多措并举提升全民数字素养与技能，以优异成绩迎接党的二十大胜利召开。

《工作要点》明确了工作目标：到 2022 年底，提升全民数字素养与技能工作取得积极进展，系统推进工作格局基本建立。数字资源供给更加丰富，全民终身数字学习体系初步构建，劳动者数字工作能力加快提升，人民群众数字生活水平不断提高，数字创新活力竞相迸发，数字安全防护屏障更加坚固，数字社会法治道德水平持续提高，全民数字素养与技能发展环境不断优化。

（来源：中国政府网）

9、《未成年人网络保护条例（征求意见稿）》公开征求意见

3 月 14 日，国家互联网信息办公室会同司法部根据《未成年人保护法》《个人信息保护法》等法律，对《未成年人网络保护条例（征求意见稿）》进行了起草修改，并再次向社会公众公开征求意见。此次《条例》草案共七章六十七条，内容上较 2016 年第一次草案内容扩充将近一倍，就未成年人信息保护、防止未成年人沉迷网络、消费管理、禁止网络欺凌等方面作出规定，并表示严禁任何组织和个人以侵害未成年人身心健康的方式干预未成年人沉迷网络、侵犯未成年人合法权益。

2016 年的草案中，关于未成年人个人信息保护的规定较少，主要聚焦于企业应合理收集未成年人个人信息、应针对未成年人个人信息制定收集规则、赋予未成年人用户及其监护人撤回同意的权利等方面。但本次草案针对未成年人个人信息保护设立了专章，从信息的收集、处理、使用、保护等方面进一步细化，与《个人信息保护法》形成呼应，填补了部分制度空白。

（来源：中国政府网）

10、《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》

1 月 24 日，国家发展改革委牵头，会同商务部、广东省、深圳市等研究制定《关于深圳建设中国特色社会主义先行示范区放宽市场准

入若干特别措施的意见》，《意见》重点提及放宽数据要素交易和跨境数据业务等相关领域市场准入，涵盖数据要素交易、数据资源产权、公共数据开放、数据安全等内容。

《意见》具体包括：一、在严控质量、具备可行业务模式前提下，审慎研究设立数据要素交易场所；二、鼓励深圳开展地方性政策研究探索，建立数据资源产权、交易流通、跨境传输、信息权益和数据安全保护等基础制度和技术标准；三、鼓励深圳市探索立法，明确处理者义务或主体参与权利，依法处理个人信息，保护数据处理者合法利益；四、加快推动公共数据开放，编制公共数据共享目录；五、开展数据跨境传输（出境）安全管理试点，建立数据安全保护能力评估认证等数据安全管理机制。六、利用区块链、量子信息等先进技术实现数据可交易、流向可追溯、安全有保障，探索建立数据要素交易领域相关标准体系；七、探索建设离岸数据交易平台。

（来源：国家发改委）

（二）地方政策法规

1、《上海市未成年人保护条例》3 月 1 日起施行

2 月 18 日，上海市十五届人大常委会第三十九次会议上表决通过了《上海市未成年人保护条例》，将于 2022 年 3 月 1 日起施行。《条例》共九章八十七条，涵盖了家庭保护、自我保护、学校保护、社会保护、网络保护、政府保护、司法保护、特别保护等内容。

围绕未成年人的个人信息保护及网络保护，《条例》进行了相应的规定。包括：任何组织或者个人**不得披露未成年人的个人隐私**。发布、转载、传播涉及未成年人的新闻报道等信息，应当客观、审慎和适度，不得虚构、夸大、歪曲有关内容，**不得违法披露未成年人的姓名、住所、单位、照片、图像以及其他可能识别未成年人身份的信息**。任何组织或者个人**处理不满十四周岁未成年人个人信息的，应当依法取得未成年人的父母或者其他监护人的同意**。未成年人的父母或者其他监护人应当按照最有利于未成年人的原则，充分考虑信息处理的目的、方式、范围以及未成年人的真实意愿，审慎作出决定。

（来源：上海市民政局）

2、《上海市推进治理数字化转型实现高效能治理行动方案》

1 月 13 日，上海市人民政府发布《上海市推进治理数字化转型实现高效能治理行动方案》。方案强调，优化安全制度保障，按照相关法律法规要求，落实数据分类分级保护、信息安全等级保护和个人信息保护制度，健全安全风险评估、安全责任落实、安全应急处置等相关机制。加强安全技术运用，探索借助区块链、隐私计算等新技术，加强公共数据安全保护技术能力。方案提出：一、明确总体要求；二、推进“三大治理”应用体系建设；三、深化“两张网”改革举措；四、夯实“一体化”数字底座；五、保障措施。

（来源：上海市人民政府）

3、《中国（上海）自由贸易试验区临港新片区条例》

2 月 18 日，上海市十五届人大常委会第三十九次会议高票表决通过了《中国（上海）自由贸易试验区临港新片区条例》，并且将于 3 月 1 日正式实施。《条例》完善了特殊经济功能区建设的四梁八柱，设总则、投资自由便利、贸易和运输自由便利、资金自由便利、人员从业自由便利和人才保障、数据流动、前沿产业发展、风险防范、权益保障、附则共十章五十五条。

其中强调，按照国家相关法律、法规的规定，在临港新片区内**探索制定低风险跨境流动数据目录，促进数据跨境安全有序流动**。支持临港新片区推进国际数据产业发展，培育发展数据经纪、数据运营、数据质量评估等新业态，建立**数据跨境流动、数据合规咨询服务、政企数据融合开发**等公共服务平台。

（来源：上海市人民政府）

4、上海市发布全市首份《企业数据合规指引》

1 月 27 日报道，上海市首份《企业数据合规指引》（下称《指引》）正式出台。据悉，《指引》由上海市杨浦区检察院联合市信息服务业行业协会、市数据合规与安全产业发展专家工作组、区工商业联合会制定发布。

此次制定发布的《指引》共有 38 条，按照合规架构与风险识别处理的逻辑划分为六章，从数据合规管理体系、数据风险识别、数据

风险评估与处置、数据合规运行与保障等方面引导企业加强数据合规管理。此次制定发布的《指引》共有 38 条，按照合规架构与风险识别处理的逻辑划分为六章，从数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障等方面引导企业加强数据合规管理。《指引》主要对企业的数据合规管理架构与风险识别处理规范作出了规定，包括**数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障**等内容，督促企业对数据进行合规管理，有效惩治预防数据违法犯罪。此外，还特别对数据刑事风险进行了提示。

（来源：上海市杨浦区人民政府）

5、上海首份《餐饮行业“扫码点餐”规范指引》

2 月 22 日，上海首个《餐饮行业“扫码点餐”规范指引》正式发布，引导经营者对相关行为进行规范。《指引》明确，餐饮服务经营者收集消费者信息应当遵循合法、正当、必要的原则，在提供扫码点餐服务时，应当限于实现处理目的的**最小范围，不得强制要求消费者对手机号、微信号等个人信息进行注册或授权，不得过度收集消费者信息**。餐饮服务经营者通过折扣或优惠的方式吸引消费者注册或授权的，应当**单独取得消费者同意**，不得与扫码点餐服务捆绑。连锁餐饮服务行业各门店之间共享消费者个人信息的，应当向消费者**告知共享范围并明确取得消费者同意**。

《指引》明确，餐饮服务经营者对已收集的消费者信息必须严格保密，**不得泄露、出售或者非法向他人提供;未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。**对于经营者违法收集消费者个人信息的，市场监管部门将按照《消费者权益保护法》等法律法规进行查处。

（来源：上海市人民政府）

6、《2022 年度天津市公共数据资源开放计划清单》

1 月 5 日，天津市委网信办、天津市大数据管理中心联合发布《2022 年度天津市公共数据资源开放计划清单》（以下简称《开放计划清单》）。

《开放计划清单》主要对标先进省市，结合重点行业、特色领域和区域特点，汇总包括信用、交通、医疗、就业、社保、教育、环境、气象、企业登记监管等民生保障服务相关领域的政务数据向社会开放。《开放计划清单》包括市级、区级两个部分。其中，市级部分收集了 47 个市级部门共 943 个开放计划目录；区级部分收集了 16 个区共 1104 个开放计划目录。

（来源：天津市信息资源统一开放平台）

7、《贵州省大数据战略行动 2022 年工作要点》

贵州省大数据发展局于 2022 年 2 月发布《贵州省大数据战略行动 2022 年工作要点》的相关通知及解读。据悉，2022 年全省大数据

工作的主要内容将从数字产业化、产业数字化、数字新基建、数字化治理、数据价值化、支撑保障 6 大方面，部署 30 项重点工作、130 项具体任务。

其中提出：着力做实数据价值化，加快打造国家数据生产要素流通核心枢纽。实施数据要素大开发行动，加快公共数据高质量归集和共享开放，推动教育、医疗、供水、供电、供气、交通等行业公共数据归集，在省属国有企事业单位建立数据专员机制。推进数据流通交易，优化提升贵阳大数据交易所，完善数据流通交易服务中心组织架构，搭建数据流通交易平台，在政务、金融、通信、电力、交通、信用等领域，培育引进一批专业“数据商”，培育数据集成、数据经纪、资产评估、定价评估、安全评估等第三方专业服务机构。开展数据要素市场化配置改革行动，探索数据市场化交易机制，研究出台支持数据要素市场培育财政制度，推进“场外交易”逐步转入“场内交易”。力争集聚数据商 300 家，形成数据产品 500 个，数据流通交易走在全国前列。

（来源：贵州省大数据发展管理局）

8、《广东省公共数据安全管理办法（征求意见稿）》

2 月 7 日，广东省政务服务数据管理局发布《广东省公共数据安全管理办法（征求意见稿）》，公开征求意见。该管理办法旨在加强广东省数字政府公共数据安全管理，规范公共数据处理活动，促进数据资源有序开发利用，保护个人、组织的合法权益，维护国家主权、

安全和发展利益。该《征求意见稿》包含总则、基础制度体系、全生命周期数据安全管理、数据安全支撑保障、监督与法律责任、附则共六章。

（来源：广东省政务服务数据管理局）

9、广东省：建设省数据交易场所和粤港澳大湾区大数据中心

2 月 28 日，广东省印发广东省数字政府改革建设 2022 年工作要点。拟全面推进**数据要素市场化配置改革**，进一步健全公共数据管理和运营体系，完善数据交易流通平台和机制，加强数据要素相关标准和技术研究，探索构建个人和法人数字空间，力争在年内取得新突破，推动数字经济创新发展。其中，拟促进数据交易流通。依托现有交易场所建设省数据交易场所，搭建**数据交易平台**。推动**数据经纪人**、“数据海关”试点。支持深圳市设立数据交易市场或依托现有交易场所开展数据交易。探索运用区块链、隐私计算等新技术**强化数据安全防护**。建设粤港澳大湾区大数据中心，健全大湾区数据基础设施体系。

（来源：广东省人民政府）

10、《浙江省公共数据条例》

1 月 21 日，浙江省十三届人大六次会议审议通过《浙江省公共数据条例》，将于 3 月 1 日起正式施行。《条例》是全国首部以公共数据为主题的地方性法规，也是保障浙江省数字化改革的基础性法规。

《条例》聚焦破解部门间信息孤岛、提升数据质量、赋能基层、保障安全等共性难题，推动浙江打造全球数字变革高地。《条例》明确了公共数据范围、平台建设规范、收集归集规则，推动公共数据有序开放，规定开放属性确定机制、明确开放范围和重点、分类开放，并明确受限开放条件和要求，助力省域治理高效协同激活数据要素市场。

（来源：浙江省人民政府）

11、《河南省数字经济促进条例》

河南省第十三届人大常委会第二十九次会议表决通过《河南省数字经济促进条例》，将于 2022 年 3 月 1 日起施行。《条例》从**数字基础设施建设、数据资源开发利用、数字产业化发展、产业数字化转型、数字化治理和服务、数字经济促进措施、数字经济安全保障和法律责任**等方面对数字经济的促进作出了规定。

条例指出，省人民政府及工业和信息化、发展改革、科技等有关部门应当统筹电子信息制造业发展，做好重大项目推进、产业链上下游对接配套、龙头骨干企业培育，打造电子信息制造优势产业集群。**县级以上人民政府应当鼓励企业开放数字化应用场景**，宣传数字经济文化，推广先进经验、成功模式。

（来源：河南省人民政府）

12、《广西加快数据要素市场化改革实施方案》

3 月 18 日，广西壮族自治区大数据发展局发布关于《广西加快

数据要素市场化改革实施方案》。方案的主要目标是：建立全区统一开放的数据要素市场；构建两层数据要素市场结构，发挥行政机制和市场机制比较优势，激发各类供需主体活力。一层市场以政府行政机制为主，通过管、建、运适度分离，建设公共数据运营平台，为数据要素流通提供保障；二层市场以市场竞争机制为主，建设各类数据交易场所，规范数据进场交易；建设三类数据要素市场化平台。围绕数据要素资源化、资产化、资本化，建设数据要素集聚平台、运营平台和交易平台，保障数据要素生产、分配、流通等各环节循环畅通；构建数据要素市场供给、流通、应用、监管“四位一体”体系，在各个行业领域探索数据要素赋能场景，释放数据要素生产力潜能。主要任务有四点：一、构建多元发展的数据要素市场供给体系；二、建立开放有序的数据要素市场流通体系；三、构建高效协同的数据要素市场应用体系；四、建立科学完备的数据要素监管体系。

（来源：广西壮族自治区人民政府）

（三）标准动态

1、《网络安全标准实践指南——网络数据分类分级指引》全文发布

2021 年 12 月 31 日，全国信息安全标准化技术委员会秘书处发布了《网络安全标准实践指南——网络数据分类分级指引》，给出了网络数据分类分级的原则、框架和方法。

数据分类分级框架中，《实践指南》提出：常见的数据分类维度包括公民个人维度、公共管理维度、信息传播维度、组织经营维度、行业领域维度；从国家数据安全角度可将数据分为一般数据、重要数据、核心数据共三个级别；建议数据处理者优先按照基本框架进行定级，在基本框架定级的基础上也可结合行业数据分类分级规则或组织生产经营需求，对一般数据进行细化分级。

（来源：信安标委）

2、《信息安全技术 重要数据识别指南（征求意见稿）》公开征求意见

1 月 13 日，全国信息安全标准化技术委员会秘书处发布了《信息安全技术 重要数据识别指南（征求意见稿）》，并面向社会公开征求意见。

该指南为 2021 年 9 月 23 日公开的标准草案《信息安全技术 重要数据识别指南（征求意见稿）》的修订版本，在框架上，新版的《指南》将旧版中“重要数据的特征”和“重要数据识别流程”合并为“重要数据的识别因素”。在内容上，新版的《指南》没有详细描述重要数据特征的小类，指提出了重要数据的十四项识别因素；此外，在识别重要数据的基本原则中，新版的《指南》将旧版中第二项“促进数据流动”原则替换为“突出保护重点”。

（来源：信安标委）

3、工信部发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》二次征求意见

2 月 10 日，工业和信息化部再次发布《工业和信息化领域数据安全管理办法（试行）》，根据此前《工业和信息化领域数据安全管理办法（试行）》（征求意见稿）收到的公开意见，工业和信息化部进行了修改完善，再次面向社会征求意见。相较于 2021 年 9 月 30 日发布的《征求意见稿》，此次《公开征求意见稿》共计八章四十一条，主要做了如下调整：目的依据中添加了《个人信息保护法》和《国家安全法》。适用数据范围扩大至工业数据、电信数据和无线电数据。对一般数据、重要数据和核心数据的定义做了调整，对备案申请时间等具体数字做出明确规定。补充了主体责任，在数据全生命周期管理方面，围绕数据出境和数据跨主体处理进行了条款补充。

（来源：工信部）

4、工信部印发《车联网网络安全和数据安全标准体系建设指南》

3 月 7 日，工业和信息化部印发《车联网网络安全和数据安全标准体系建设指南》，提出到 2023 年底，初步构建起车联网网络安全和数据安全标准体系。重点研究基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等标准，完成 50 项以上急需标准的研制。到 2025 年，形成较为完善的车联网网

络安全和数据安全标准体系。完成 100 项以上标准的研制，提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平，支撑车联网产业安全健康发展。

（来源：工信部）

5、《智能网联汽车数据安全评估指南》公开征求意见

3 月 9 日，由国家工业信息安全发展研究中心牵头编制的《智能网联汽车数据安全评估指南》团体标准(以下简称“标准”)正式公开征求意见。标准旨在进一步落实《汽车数据安全管理若干规定》《车联网网络安全和数据安全标准体系建设指南》等政策法规要求，不断优化标准供给结构，提高行业服务能力，对规范智能网联汽车行业数据处理行为具有重要意义。

智能网联汽车数据安全评估主要有数据安全风险评估、数据安全合规性评估和数据出境安全评估三种类型。本标准规定了智能网联汽车数据安全评估的技术要求，共分为八部分，包括范围、规范性引用文件、术语和定义、数据安全风险评估实施流程、数据安全合规性评估实施流程、数据安全评估结果、参考文献、附件内容。

（来源：国家信息安全发展研究中心）

6、浙江省发布《公共数据元管理规范》省级地方标准

1 月 12 日，浙江省市场监督管理局批准发布了 DB33/T2426-2022《公共数据元管理规范》省级地方标准。该标准规定了公共数据元的

属性、构成和管理的要求，标准适用于各级机关、团体、企事业单位、社会组织等公共管理和服务机构开展公共数据元的管理与使用工作。

该标准明确了公共数据元属性：基础属性和扩展属性，明确了公共数据元分类：自然人类、法人类、信用类、自然地理类、感知类、统计类和其他类，明确了公共数据元关系：派生关系、组成关系、替代关系和连用关系。

（来源：浙江省市场监督管理局）

7、首个隐私保护机器学习国际标准正式推行

1 月 11 日消息， IEEE 标准委员会正式发布并推行了基于可信执行环境的隐私保护机器学习的国际标准（IEEE Std 2830™）。这也是国际上首个基于可信执行环境的隐私保护机器学习技术框架与要求的国际标准。由蚂蚁集团联合国内外共知名高校、研究机构共同立项、筹备、制定。该标准的设立通过规范隐私计算的技术标准，为保护数据隐私和释放数据价值提供了可落地的技术标准方案。

此标准的制定可用以指导规避隐私计算技术体系中存在的风险，促进多个数据提供方在满足数据安全、隐私保护和监管合规等要求下，实现基于数据协同和授权共享的数据聚合和计算，在保护保护数据隐私的基础上释放数据价值。

（来源：央广网）

二、两会声音

（一）数据安全

1、加强我国跨境数据流动监管

全国政协委员、中国工程院院士 陈晓红

数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。建议加强我国跨境数据流动监管，完善跨境数据流动管辖法律法规体系。

一是完善跨境数据流动管辖法律法规体系。构建跨境数据流动监管的国际互信机制，开展数据出境安全评估、数据保护能力认证、标准合同条款、“白名单”等机制建设。同时，要健全数据出境安全评估配套措施。

二是推进数据跨境流动安全保障能力建设。要加强数据安全风险评估、追踪溯源、监测预警等技术能力建设，支持数据跨境流动安全保障技术研发。同时，建立数据全生命周期安全保护责任制度。

三是强化跨境数据流动安全的内审机制建设。加强数据安全保护法治教育，提高企业敏感数据合规管理意识；加强对数据输出方的监管，加强数据安全风险监测和评估，建立数据泄露等安全事件的应急响应机制；建立数据接收方资格审查等监管机制。

四是积极推进数据跨境流动中国治理方案。要积极加入 APEC 框架下的 GDPR 体系建设；主动参与数据跨境流动的多边或双边协定

谈判；充分利用“一带一路”建设契机，在数字经济治理上及时提出中国方案，发出中国声音。

五是建议构建统合跨境数据监管职权与技术资源的新机制。对敏感个人数据、商业数据、国家安全敏感数据及关键基础设施信息建立分级分类管理制度；要明确包括第三方数据交易机构、数据源机构等在内的数据交易主体的资质和权责，制定跨境数据交易规则等。

（来源：光明网）

2、网络安全升级为数字安全，筑牢数字安全屏障

全国政协委员、360 集团创始人、董事长兼 CEO 周鸿祎

我国数字安全投入占比在全球范围内相对较低，发达国家仅网络安全占整体 IT 的投入比例达 10%，而我国尚不足 1%。究其原因是部分政企单位仅依照合规堆砌产品，缺乏实战能力，缺乏科学能力评估。周鸿祎指出，互联网下半场，主题是产业互联网，主角是政府和传统企业，传统产业经过数字化再造后，会面临新的安全风险挑战。

与此同时，数字化新技术、新应用的产生，也导致简单安全问题升级为复杂安全问题。比如大数据、云计算、人工智能等大量新技术的使用，除了网络安全外，会带来大数据安全、云安全、供应链安全、区块链安全等一系列全新复杂安全挑战。

周鸿祎建议将**网络安全升级为数字安全，建立保障数字经济发展、护航数字中国建设的数字安全屏障体系**。

基于此，周鸿祎提出三点建议，一是瞄准产业数字化新场景，同步规划建设行业数字安全体系，保障传统产业数字化转型；二是要面向新型数字技术和应用场景，研究建设前瞻性的数字安全平台体系；三是建议以城市为主体，由政府统筹打造城市级数字空间安全基础设施和应急体系，保障经济社会稳定发展。

（来源：新华网）

3、警惕网络司法拍卖资本化垄断倾向蕴含的数据和资金安全风险

全国人大代表、上海市徐汇区委书记 曹立强

目前，电商平台所占份额已呈现相当明显的集聚性。部分平台逐渐暴露出数据安全与资金安全风险、平台间无序竞争等问题，亟须引起高度重视。为实现依法、公开、公平、便民的司法拍卖工作目标，曹立强建议，最高人民法院细化网络司法拍卖中涉及反垄断、金融安全、数据安全的法律规范和实施意见，并在实施过程中与相关部门（如市场监管局、中国人民银行、网信办）寻求配合和协同。

一是加强司法拍卖的数据安全监管。建议高度重视网拍平台可能存在的数据安全问题，尤其关注部分网拍平台以提供增值服务等名义，将其获取的案件、用户信息等与中介服务机构共享的情况，防范信息滥用风险，加强对网拍平台数据安全和信息使用的监管以及辅助机构信息保密的监管。同时，要求网拍平台应尽到数据安全义务，杜绝数

据泄露和信息滥用，防范非授权机构以此侵犯公民隐私权利，损害司法拍卖形象。

二是加强司法拍卖的资金安全监管。建议持续健全完善资金安全监管体系，对资金流转过程中的违规行为予以坚决整改，加强对收取拍卖款项账户的监管力度，确保资金安全。在选择拍卖平台时，加强平台情况审核，不得委托信誉较差的平台实施网拍。对于平台允许竞买人“赊钱”（贷款）缴纳保险金的现象，应严格限制借贷交保的条件，加强竞拍人商业信誉的审查，对涉案较多、争议频发的竞拍人依法采取限制措施，防止出现竞买人盲目竞标、房产“首付贷”的现象。

三是建议防范司法拍卖领域资本无序扩张。不断健全多层次的竞争监管规则体系，加强平台选择的公平性和透明度，着力查处资本无序扩张、平台垄断等背后的腐败行为。完善现有公共司法拍卖平台，与公共资源交易平台探索实现数据对接、监管对接。以上海为例，司法拍卖已被上海市政府列入公共资源交易目录，建议参照上海模式，坚持“一网交易”“一网监管”“应进必进”原则，建立全流程留痕、实时监管系统，从而保障司法拍卖高质量运行。同时，进一步扩大网拍平台数量，在实施拍卖选择平台时，建立委托平衡机制，实现各平台承担网上拍卖的相对平衡。

（来源：新浪财经）

4、应设立网络安全和数据保护窗口

全国政协委员、天达共和律师事务所主任 李大进

近年来，网络安全与数据保护领域的立法正处于活跃期，企业在面对大量法律法规及指导文件时，难以准确把握相关要求的落实；同时日益完善的个人信息保护制度赋予了其广泛的权利，但在行使权利的过程中却无法及时得到有效的反馈与响应。李大进建议：

一是加强履行相关职责部门之间的统筹和协调。在打破部门界限，形成监管合力的同时，也应当明晰统筹工作的具体内涵外延；

二是设立网络安全和数据保护的窗口提供指导咨询服务。对于涉及不同主管部门的咨询内容，窗口应该具备能力进行内部的资源共享、协调统合，通过统一窗口给出权威的答复；

三是尽快落实和明晰个人信息保护投诉、举报渠道和方式。公开投诉举报渠道，对于投诉举报的问题应当依法进行处理并公示相关结果。李大进认为，“这样既能彰显法律规定的威慑效力，同时也是监管部门借助社会力量广泛掌握实际情况，提高监管工作效率的有效途径。”

（来源：中新经纬）

5、仍有数据处理主体合规能力欠缺，可发挥第三方专业机构作用

全国政协委员、重庆静昇律师事务所主任 彭静

2021 年《数据安全法》、《个人信息保护法》实施后，对数据处理者提出更高的合规要求，需建立并完善一整套数据处理机制，但不少数据处理主体数据合规意识淡薄、合规能力欠缺。

全国政协委员彭静建议，对数据治理、保护能力进行梳理，在各级党委、各地国有资产监督管理部门统一部署下，梳理数据保护重点行业、从事高风险数据处理活动的政府机关、国有企业，应当明确对外委托专业机构开展数据合规工作的类型。其次建立对外委托工作流程、考核机制，建立专业机构资质入库机制。

同时，彭静建议制定个人信息保护合规标准，保障第三方合规工作质量。她进一步指出，银行保险、证券、市场、卫生健康等行业监管机关应鼓励、采纳本行业协会、企业编制符合本行业实际与发展的数据保护行业标准及第三方合规工作认证机制。

彭静认为相关监管机关应与人民法院、人民检察院建立联席工作机制，实现相关行业第三方数据合规标准与《关于建立涉案企业合规第三方监督评估机制的指导意见》等司法合规制度无缝对接，确保第三方合规工作成果法律效力，整合企业事前、事后一体化数据合规能力。

（来源：21 财经）

6、升级数据安全管理模式，加强关键数据管控

全国政协委员、上海市信息安全行业协会名誉会长 谈剑锋

目前我国数据安全立法体系已逐步完善，但面向特定领域的基础性数据安全体系建设尚有不足，如生物特征数据管控、医疗健康数据管理等尤为突出。我国新型生物特征数据现阶段主要由企业掌握。如果不将这些数据集中收储管理，将导致数据要素价值受限；数据使用难以管控，滥采滥用与数据垄断并存；数据安全难以保障；数据安全执法不易，屡见多头管理、管不到位的现象。

对此，谈剑锋建议，细化相关法规制度，以点带面明确数据权属，提高数据安全执法的可操作性。明确已汇聚的生物特征数据等为公共产品，参照“重要数据”来管理，达到一定数量还应被视作核心数据。

同时，尽快设立国家“数据银行”，由国家成立专门机构统一管控，以最大程度地保障关键数据安全和国家安全。国家“数据银行”优先收储个人生物特征、医疗健康数据等具有唯一性、不可再生性的数据，按需提供数据应用，严格审计，保证向个人开放数据使用查询。

另外，他还建议，促进安全技术发展，夯实安全产业基础，增强数据治理能力和数据监管水平。加快建设数字身份基础设施，围绕身份识别与信任，解决数字空间中的身份认证与治理相关的核心技术问题。

（来源：南方都市报）

（二）个人信息保护

1、进一步完善个人信息保护

全国政协委员、致公党上海市委专职副主委 马进

近年来，个人信息保护一直是人们关注的焦点。虽然近年来关于个人信息保护方面的立法工作取得了很大进展，但在具体推进中仍存在以下主要问题：平台、经营者的相关责任义务尚未细化明确，相关主体责任意识缺位，导致非法设备泛滥；“告知一同意”机制徒具形式，相关隐私保护条款往往以冗长模糊、暗设陷阱等面目示人，异化为空头支票乃至避责手续，而消费者只能被动同意；个人信息被泄露的途径层出不穷，如何准确、有效、快速地举证、维权成了一大难题。

马进委员建议，为加快完善立法，尽快建立健全互联网时代个人信息保护。

首先，明确平台、经营者的法定责任和义务，压实主体责任。应进一步完善法律法规细则，明确网络第三方平台，酒店、宾馆等公共场所，相关电子设备生产经营商家等在个人信息采集、传输、存储、使用等生命周期各环节的主体责任和义务。建立事后追责机制，加大对信息泄露等相关违法行为的查处和处罚力度，倒逼相关主体加强内部管理，不再对个人信息保护不力存有侥幸心理。

同时，细化“告知一同意”机制，保障知情、监督等权利真正落地。告知同意是个人信息处理规则的核心，应进一步完善法律法规细则，要求相关隐私保护条款或终端使用者授权合约的设立应以简明、醒目

的方式明确使用者的权利、义务以及个人信息的被使用范围等重要内容，不得滥用合约权利设置冗长模糊的条款诱导使用者被动同意，甚至暗设陷阱。

此外，进一步降低受害者维权门槛，切实保障公民应有权益。关于个人信息被侵害，按照现行的侵权责任归责体系及构成要件，原告应举证证明其因对方原因而遭受损害或损失。而根据《个人信息保护法（草案）》第六十五条规定，个人因此受到的损失或个人处理者因此获得的利益难以确定的，由人民法院根据实际情况确定赔偿数额，但其在实际操作中仍有不足。应通过立法进一步细化纠纷处理机制，完善权利救济渠道，同时加重被告的举证责任，以督促掌握个人信息的机构或组织妥善合法获取个人信息。

（来源：人民日报）

2、多措并举加强个人信息司法保护

全国政协委员、陕西省人民检察院副检察长 高洁

如何有效整治个人信息被窃取、泄露和滥用的现象，如何精准打击因个人信息泄露导致的网络违法犯罪行为，是我国未来在加强个人信息司法保护时需重点关注的方面。行业平台内部监管仍存在漏洞是个人信息被窃取、泄露和滥用的重要原因之一。

高洁建议，加强个人信息司法保护，需要执法、司法和检察部门形成综合合力。就执法司法机关而言，要坚持全链条惩治，将惩治侵

犯公民个人信息纳入打击治理网络犯罪特别是电信网络诈骗犯罪中加以部署推进。对行业和企业‘内鬼’泄露个人信息的行为要加大刑事处罚力度，形成有力震慑。检察机关应发挥刑事检察和公益诉讼检察的双向合力，推动个人信息保护源头治理。要重点聚焦侵害个人敏感信息、特殊群体个人信息以及大规模个人信息案件，关注重点行业部门和大型平台企业，加大公益诉讼力度，形成有力声势。

结合司法办案，还应积极推动涉案企业加强合规建设，特别是推动数据合规建设。例如，可通过引入第三方监督评估机制，督促涉案企业做到真整改、真合规，筑牢用户个人信息保护的闸门。

此外，持续深化行业教育和社会警示对于在全社会形成保护个人信息的良好氛围具有重要意义。应借助以案释法、曝光典型案例等方式，加强法律宣传教育，提升个人信息保护法治意识，推动和助力网络强国建设。

（来源：人民网）

3、加强快递业个人信息保护刻不容缓

全国政协委员、上海市政府参事、上海中华职业教育社常务副主任

胡卫

2021 年，我国快递行业年发件量正式迈入“千亿件时代”，快递成为连接千家万户的必需品。不过，在提供便利的同时，因快递面单导致个人信息泄漏的事件频发，也使得加强个人信息安全保护的呼声越

来越高。造成这种局面的主要原因在于：利益勾连导致个人信息贩卖活动屡禁不止；快递企业寄递服务信息安保机制不健全；同时，存在相关监管部门对快递行业个人信息泄露问题查处不力的现象。

对此胡卫提出几点建议：

（1）及时修订《快递暂行条例》及《寄递服务用户个人信息安全管理规定》，从而强化其中的法律责任，为快递业个人信息保护提供更为坚实的法制保障；

（2）建立健全常态化日常监管制度。进一步完善对快递企业的定期巡检和飞行检查制度，督促快递企业将个人信息保护落实到内部管理全流程、各环节；

（3）相关部门要切实加大执法力度；

（4）加强技术防护和安全教育。

（来源：腾讯网）

4、加强电子废旧物循环利用中的个人数据安全保障

全国人大代表、小米集团董事长兼 CEO 雷军

我国是电子产品的制造大国和消费大国，也是电子产品的废弃大国。据《中国废弃电器电子产品回收处理及综合利用行业白皮书 2020》，现阶段我国每年电子废旧物处理量已达到 8000 万台左右。另外一则数据显示，目前我国规范回收率不足 20%，而欧洲已达到 42.5%。加强电子废旧物循环利用体系建设，对于保障国家资源安全、推动实现“双碳”目标具有重要意义。

对此，雷军提出四点建议：**一是制定电子废旧物循环利用中长期发展规划；二是大力培育市场主体，加强协同规范发展；三是保障个人数据信息安全，提升电子废旧物回收率。**据统计，2020 年我国居民手机保有量已高达 12.6 亿台。当前，公众对信息泄露风险的担忧也不断加深，在一定程度上导致了电子废旧物回收率难以实现大幅提升，建议在电子废旧物循环利用各环节中，严格落实个人信息保护操作规范，打通个人信息安全的“最后一公里”，有效提升电子废旧物回收率；**四是加强宣传引导，开展个人电子废旧物碳积分试点，便于查询个人电子废旧物流通信息，展示个人碳积分及排名信息等，适时向全国推广，提高公众参与度。**

（来源：C114 通信网）

5、依法从严打击侵犯公民个人信息犯罪

全国人大代表、九三学社中央法律委员会主任、北京市信利律师事务所律师 阎建国

在整个黑色产业链中，非法收集和利用个人信息是其中的重要一环，是多数网络犯罪实施的源头行为，在大多数电信网络诈骗犯罪中，犯罪分子或是通过非法获取的公民个人信息注册手机卡、银行卡，以此作为诈骗犯罪的基础工具，或是利用这些信息对诈骗对象进行“画像”实施精准诈骗，危害十分严重。

阎建国建议**坚持全链条惩治，依法从严打击侵犯公民个人信息犯罪。**坚持“一案双查”，在查办下游网络犯罪的同时，溯源上游个人信

息泄露的渠道和人员，围绕信息获取、流通、使用等各环节，同步加强全链条打击。加大对行业“内鬼”泄露个人信息行为的刑事处罚力度，形成有力震慑。

同时，**发挥刑事检察和公益诉讼检察双向合力，切实加强公民个人信息的公益保护。**认真落实个人信息保护法有关规定，刑事检察和公益诉讼检察部门要加强协作配合，强化信息互通、资源共享、线索移送、人员协作和办案联动，对于重大案件，探索建立联合办案组，发挥刑事检察和公益诉讼检察双向合力，推动个人信息保护源头治理。

结合司法办案，**推动涉案企业加强合规建设特别是数据合规，引入第三方监督评估机制**，对于“个人敏感信息、个人信息和其他信息”“特殊群体、特定对象、重点领域”个人信息建立分级保护制度；对于持续批量、短时间内大量获取个人信息等异常行为加强技术监控、预警和阻断；对于重点岗位人员、分支网点人员、离职人员从严加强管理，督促涉案企业“真整改”“真合规”。

（来源：中国人大网）

（三）数据要素与数据确权

1、加快数据确权立法解释和配套法规政策，促进和保障数字经济健康有序发展

北京市朝阳区政协副主席、北京国际城市发展研究院院长 连玉明

随着《民法典》《数据安全法》《个人信息保护法》相继出台实施，从不同角度确立了数据和数据权的法律地位，为数字经济健康有序发展提供了基础制度支撑。但最为关键、最为核心和最为基本的数据确权问题一直没有解决。为此，连玉明建议：

一是针对数据确权的基础性问题作出立法解释。包括对数据和信息的内涵外延，数据和信息究竟是利益、法益或是权利等作出法律解释。要进一步规范统一立法术语，完善立法语言技术，明确数据确权范畴，使整个数据法律体系内各术语之间表述一致、完整准确，各项规定之间相互衔接、相互协调。

二是尽快制定关于数据确权的行政法规和配套政策。现行法律关于数据的规定较为笼统，大多是概括性、原则性甚至宣示性的规定，有些条款尚停留在理念和呼吁层面。数据确权制度需要细化，才具有可操作性和可适用性。建议加快推动数据确权行政法规、部门规章和规范性文件出台，配套推出相关条例、办法、规定、通知；研究制定数据分类分级标准，建立基于场景化或类型化的数据确权模式；建立健全数据确权、授权、采集、开发、定价、交易、利用、分配生态体系中的数据伦理治理体制。同时，明确国家和地方各级数据确权主管和协调、监管和执法机构职责，从定机构、定职能、定编制、定数据“四定”对部门进行数据确权定责，出台部门数据权责清单。

三是加快出台关于数据确权的司法解释。进一步细化数据分级分类确权制度。按照个人数据和非个人数据、公共数据和非公共数据、原始数据和衍生数据的划分进行权属总体确认。

（来源：和讯新闻）

2、加快培育数据要素市场，助力数字经济做强做优做大

全国人大代表、上海移动总经理 陈力

近几年，随着《数据安全法》和《个人信息保护法》陆续出台生效和《网络安全审查办法》进一步修订，关于加强数字经济治理的法律法规和政策制度体系不断健全，但仍存在着一些影响数字经济健康发展的问题。陈力代表认为，在不断深化挖掘数据要素的过程中，应坚决纠正和解决一些平台垄断、信息安全、用户权益等方面不健康、不规范的苗头，方能发挥数据作为生产要素作用，保证数据要素市场的健康有序发展。因此，建议从以下六个方面予以加快培育数据要素市场：

一是推进数据要素市场统筹规划，需要在政府的调控和监管之下，统筹企业、社会多方力量，多管齐下地推进数据市场化配置。二是健全数据生产要素发展和交易基础，在明确产权的基础上形成数据要素按市场评价贡献、按贡献决定报酬的初次分配基本框架，制定通过财税工具完善再分配的政策体系。三是确立数据分类分级管理制度，梳理出各个行业领域的不同种类数据，并筛选出非敏感、低风险等级、权属相对明确的数据资源，以要素形式优先进入数据交易市场，高效配置数据资源。四是提升数据质量全力开发数据生产要素应用场景，通过市场需求激发服务主体动力，打好数据质量评价和应用的基础性工作，建立数据质量管理体系，实现大数据的质量目标。五是构建数

据要素开放共享格局，包括推动政府公共数据开放共享形成示范效应、整合各类数据发挥数据要素的协同效应等。六是健全数据要素安全保障机制，根据数据分级对数据进行强制加密，建立数据访问管理规则，设置管控权限，防止内部数据外泄。

（来源：中国日报）

3、建议制定数字经济促进法、数据产权法

全国政协委员、北京金台律师事务所主任 皮剑龙

我国数字经济发展存在缺乏统筹设计，法律制度供给不足，立法结构和体系过于分散，数字经济管理体制机制不健全等问题。具体来说，现有数字经济管理机构和权限比较分散，尚未建立统一的数字经济治理框架和规则体系，机制的系统性、管理的及时性和制度措施的科学性都有待加强。另一方面，我国数字经济基本法律缺位——尤其关于数据产权等核心问题。

因此，皮剑龙建议**设立“国家数字经济工作局”**，作为中央统筹数字经济发展的管理协调机构，主要职能包括：统筹谋划全国数字经济发展，组织实施数字经济建设；指导推进数字政府建设、各行业领域信息化建设、新型基础设施体系构建；加强数字产业监管，对公共数据实行集中管理；对数字经济领域人财物资源进行统筹安排；提升政府服务效能，在更高层次更高水平上释放和促进数字经济生产力，调整和适应数字经济生产关系，服务和促进数字经济生产关系发展。

数据产权问题是数字经济发展中的核心问题之一，但我国缺乏相关法规。对此，他建议加快制定《数据产权法》，在其中明确合法、公平、效率等原则，确定数据所有权、支配权、使用权、收益权等权利的归属，与数据产权的流通和交易规范，以此增强市场主体对数据利益的可期待性和市场信心。

（来源：南方都市报）

4、制定与修改数据资产流通相关法律法规

全国人大代表、海尔集团董事局主席、首席执行官 周云杰

数字经济正在成为重组全球要素资源、重塑全球经济结构、改变全球竞争格局的关键力量。在数字经济时代，数据成为关键性生产要素，安全有效地推动数据利用、共享和流通，挖掘数据价值，将快速释放数据生产力，助推经济社会高质量发展。

我国现行数据保护相关法律落点于数据安全，相关立法仍有不足。数据交易面临着确权难、定价难、互信难、入场难、监管难的“五难”问题。因此，周云杰提出制定与修改数据资产流通相关法律法规的议案。具体建议为：

颁布数据产权保护相关的法律法规，加快推进数据资产确权。完善数据资产价值的相关会计准则，为以数据资产进行的出资和交易奠定基础。建立全国性数据交易平台，制定统一的数据交易市场规则及标准，组建数据交易监管职能部门。

（来源：搜狐新闻）

5、明确数据权属，规范交易活动

全国人大代表、民建中央委员、民建广东省委会副主委、华南师范大学教授 林勇

数据已经成为数字经济时代最为核心的生产要素之一。而要充分发挥数据要素价值、驱动产业变革，必须推动数据便捷流动、共享利用，实现数据要素市场化配置。但目前我国在数据交易方面还存在许多问题。

林勇建议**推动数据交易领域立法**。研究制定《数据交易法》，重点明确交易范围、数据权益、配套支持和监管方式。大胆尝试、逐步完善、严格监管的原则，在《数据交易法》立法前后，通过制定配套行政法规或部门规章的形式，出台有关数据交易的制度规范。

同时也要**构建数据监管治理体系**。完善制度保障，构建数据监管治理平台技术支撑体系，探索数据要素监管“沙盒模式”。以组建行业联盟的形式搭建政府和企业沟通桥梁，制定行规行约和各类标准。支持企业在政府和行业框架下建立企业标准，强化交易主体责任。

要明确数据所有权、使用权、处理权、控制权、收益权等各种权利属性，确定各种数据权拥有者的相关权责。对涉及个人隐私、商业秘密和国家安全等数据在大数据营销、企业数据共享、数据跨境流动、政府社会治理、公共服务、公共安全应用等特定使用场景下进行使用约束，避免隐私权与财产性数据权属混同。

（来源：搜狐新闻）

（四）东数西算

1、全面推进“数利”基础设施建设，助力国家“东数西算”战略实施

全国政协委员、启明星辰集团首席执行官 严望佳

东数西算”作为数字经济的基础设施，在对接地方经济和产业经济领域等方面必须有对应的政策机制和发展指引。建议借鉴水利基础设施模式，针对数据要素建设“数利”基础设施，从而形成“数据流域化大格局”，如同水系流域一样将数据要素分布在数据流域内，让数据要素像水一样安全、顺畅地流淌在“数利”基础设施内，可以像使用水力和电力一样安全、便捷地使用数据要素。

对此，严望佳建议：

（1）准确把握规律，积极开展理论研究和实践。深究数据要素化基本规律，积极开展数据流域化发展实践，破解数据跨区域、跨部门安全流通与应用难题，打通数据要素流通壁垒，推动数据流域内产业数字化和数字产业化转型升级。同步研究建立安全相关基础设施，打造纵深协同、安全可信的网络安全运营体系、数据安全运营体系、云网边端数用一体化安全体系，支撑数利基础设施迭代优化和安全可持续发展。

（2）以城市为支点，全面推进数利基础设施建设。以“东数西算”的八大枢纽和十大集群为核心，结合地方智慧城市群规划，建构区域化的数据流域化格局，这些数利基础设施包括但不限于：**城市级算力基础设施（城市公共数据中心），城市数据流通交换交易基础设施，城市级网络安全运营中心基础设施，城市级数据安全治理基础设施，城市级数据灾备中心基础设施，城市级云网融合边缘安全接入基础设施**等。

（3）以主力行业和产业链为支点，全面推进数利基础设施建设。贯通“东数西算”八大枢纽和十大集群，从数据流域化格局看，不仅仅有围绕城市的区域流通格局，还有围绕产业链的行业流通格局。在这个过程中重视数据驱动产业全价值链运营，建构产业化和行业化的数据流域化格局。这些数利基础设施包括但不限于：**行业级算力基础设施，行业数据流通交换交易基础设施，行业网络安全运营中心基础设施，行业级数据安全治理基础设施，行业级数据灾备中心，结合行业特色的算力基础设施或数据基础设施**等。

（来源：搜狐新闻）

2、“东数西算”工程为企业提供发展新契机

全国政协委员、佳都科技集团董事长 刘伟

以新网络、新设施、新平台、新终端为代表的数字‘新基建’对能源需求强大，本身就是耗能大户，在建设过程中应特别注意自身的能耗需求，因此刘伟认为新基建加速发展要算好‘自身能耗账’。“东数

西算”工程是优化全国数据中心建设布局的重要举措，东部地区土地、能源等资源日趋紧张，难以大规模发展数据中心。将东部算力需求有序引导到西部，可以充分发挥西部地区人口密度低、太阳能和水电资源丰富、土地广阔等优势，缓解东部数据中心的发展压力，有效降低东部碳排放并促进东西部协同联动，将为相关企业提供发展契机。

针对企业应如何融入“东数西算”新机遇，刘伟提出四点建议，一是加强核心技术与自主产品研发的投入力度，提升产学研合作水平和科技成果转化效率。二是创新研发体系，打造 AI 中台，不断提高产品标准化程度。三是摸索更优的 AI 落地场景和商业模型。四是做好定位和规划，加大创新投入，融入数字经济建设大局。

（来源：赛迪网）

3、加快算力网络创新发展 构筑国家竞争新优势

全国人大代表、中国移动董事长 杨杰

算力是继热力、电力之后新的关键生产力，已成为衡量一个国家数字经济发展水平的重要指标。加快提升国家整体算力水平，对加强国家综合实力、构筑国家竞争新优势具有重大意义。在这一背景下，如何推动算力的高质量发展？这需要充分发挥中国在网络领域的积累，加快算力网络创新发展，推动算力成为像水、电一样，可“一点接入、即取即用”的社会级服务。

如何破解算力网络发展难题，提升中国在算力领域的综合竞争力？杨杰从顶层设计、技术创新、产业推进、应用孵化、配套政策等方面提出五点建议。

一是加强顶层设计和统筹布局。二是建强原始创新策源能力。三是加快推动配套产业成熟。 四是培育壮大算力网络应用生态。五是加快完善配套政策支持体系。

（来源：时刻新闻）

4、建议在中部部署算力网络国家枢纽节点

全国人大代表、河南移动总经理 杨剑宇

为抢抓新一轮科技革命和产业变革新机遇，推动数字经济加快做强做优做大，国家启动了“东数西算”工程，通过建立横跨东西的算力网络与数据存算一体化节点，推动数据中心合理布局、供需平衡、绿色集约和互联互通。2021 年国家发展改革委、中央网信办、工业和信息化部、国家能源局联合印发了《全国一体化大数据中心协同创新体系算力枢纽实施方案》，提出在京津冀、长三角、粤港澳大湾区、成渝，以及贵州、内蒙古、甘肃、宁夏等地布局建设全国一体化算力网络国家枢纽节点。方案同时指出，根据发展需要，后续适时增加国家枢纽节点。

对此，杨剑宇建议在中部部署算力网络国家枢纽节点，促进中部地区数字经济发展。优化“东数西算”网络结构，实施东、中、西部区域梯次布局，在中部增加算力网络国家枢纽节点。

中部地区数字经济发展需要算力枢纽设施，同时，在中部部署国家枢纽节点也能为全国尤其是东部地区提供高品质、低成本温数据算力需求保障。通过在中部部署国家枢纽节点，优化“东数西算”网络结构，将有助于构建布局更加合理、技术经济更具相对优势的算力设施新格局，为构建国内大循环、实现东中西部数字经济协调发展发挥更好的支撑作用。

（来源：人民网）

三、技术、产品与市场洞察

（一）技术与产品

1、谷歌宣布推出 Android 隐私沙盒，计划年内发布开发者预览版

2 月 16 日消息，谷歌宣布推出 Android 隐私沙盒，旨在引入更新、更具私密性的广告解决方案，以限制与第三方机构共享用户信息，但却不损害广告主短期利益。据介绍，谷歌计划在年内随测试版一起发布隐私沙盒开发者预览版。

此次推出的隐私沙盒建立在 Android 已有的网页端基础之上，为改善 Android 隐私提供了一条清晰的路径，同时又不会影响用户对免费内容和服务的访问。据介绍，开发者已可以在 Android 开发者网站查看隐私沙盒的初始设计方案并且分享反馈。谷歌计划在年内，随测试版一起发布开发者预览版。

（来源：安全内参）

2、国内首个！隐私计算类金融应用产品纳入国推认证

2 月 9 日，市场监管总局联合人民银行发布《金融科技产品认证目录（第二批）》，多方安全计算金融应用产品被重磅纳入，引起行业热议！**这是隐私计算领域首个被纳入国推认证的产品类型。**

根据认证规则，多方安全计算金融应用产品认证依据被指定为 2020 年中国人民银行正式发布的《多方安全计算金融应用技术规范》

(JR/T0196-2020)金融行业标准、2021 年中国支付清算协会发布的《多方安全计算金融应用评估规范》(T/PCAC0009-2021)标准。此外，认证规则规定了金融科技产品认证的基本认证模式为：型式试验+获证后监督。

（来源：开放隐私计算公众号）

3、Gartner：IAM 技术发展六大趋势

由于数字业务依赖 IAM 赋能的数字信任，安全和身份管理成为企业业务生态系统的重要基础。日前，Gartner 列出了 IAM 技术发展的六大趋势，企业可以参考其完善已部署的 IAM，以更好地满足不断变化的需求。

（1）更智能化的访问控制

（2）更好的用户体验

（3）将设备身份统一纳管

（4）实施 API 安全控制

（5）适配多云环境

（6）更完善的 IGA（身份治理和管理）功能

（来源：安全牛）

4、微软洞察：身份管理漏洞成为数字安全首要威胁

确保身份认证及管理的安全性是确保数字安全的重中之重。当今世界，身份认证已经成为关乎每个人工作生活方方面面的关键凭证，

“身份”背后存储的是每个人在浩如烟海的各类应用和服务中的全部记录。正是因为身份认证如此重要，如果没有对身份认证加以正确的安全保护，将带来巨大的潜在风险。目前以多因素认证（MFA）、无密码方案为代表的强身份认证的使用率还很低——而那些仅仅依靠密码保护的账号，常常成为黑客们最容易得手的目标。

微软数据显示，截至 2021 年 12 月，在采用微软云端身份解决方案 Azure Active Directory（AAD）的各行业客户中，只有 22%启用了强身份认证保护措施。仅在 2021 年 1 月到 12 月的一年里，微软就阻止了 256 亿次针对 AAD 的暴力破解身份认证攻击，并通过 Microsoft Defender for Office 365 拦截了 357 亿封网络钓鱼电子邮件。

对于大多数组织来说，以多因素认证、无密码解决等方案强化身份管理，是防范各种类型安全威胁，最行之有效又简便易行的重要手段。企业和组织可以通过以下方式更好地保护自己：**（1）启用多因素身份验证（MFA）；（2）审核账户权限；（3）审查、强化和监视所有租户管理员账户；（4）建立并实施安全基线以降低风险。**

（来源：freebuf）

（二）市场洞察

1、企业数据泄露防护 (DLP) 市场年复合增长高达 21%

根据 Research And Markets 最新发布的调查数据，未来五年全球企业数据泄露防护（DLP）市场预计将以 21.03%的复合年增长率高速

增长，到 **2026 年市场规模将达到 62.65 亿美元**，而 2019 年为 16.47 亿美元。

DLP 解决方案可按照网络、存储/数据中心、端点、服务、咨询、系统集成、培训等不同应用领域进行分类。根据部署模式，DLP 还可分为内部部署和云端防护两大类。由于云数据丢失防护为电子邮件、USB 驱动程序、笔记本电脑和移动电话提供了解决方案，因此预计云 DLP 细分市场将会进一步增长。

从垂直行业来看，新兴行业中越来越多地开始使用企业数据丢失防护，此外，航空航天和国防、通信和技术、政府、医疗、制造和其他行业的 DLP 市场也将以高复合年增长率增长。

（来源：安全内参）

2、Gartner 报告：2022 年法律、合规和隐私领导者的首要任务

近日，Gartner 发布《2022 年法律、合规和隐私领导者的首要任务》，通过对**高级律师、法律运营，合规和隐私高管**面临的常见挑战进行民意调查，了解法律和合规领导者在 2022 年重点关注方向和首要任务。

根据 2022 年 Gartner 法律与合规高管优先事项调查，法律、合规和隐私领导者在 2022 年需要解决的五大挑战依次为：**被日常需求限制的战略效益；第三方风险管理的复杂性超越了治理和技术的实施速度；合规计划没有跟上利益相关者的期望（例如 ESG、DEI）；隐私**

政策和程序没有与不断变化的隐私法规保持同步；跟踪监管变化的工具杂乱无章且效率低下。

（来源；赛博研究院公众号）

3、Forrester：第三方风险管理市场将“百花齐放”

研究咨询公司 Forrester 在最新发布的《Now Tech：第三方风险管理平台，2022 年第一季度》报告中称，第三方风险管理（TPRM）在业务优先级和风险管理优先级列表中位居前列，并将呈现“百花齐放”的发展态势。

目前，有几类供应商支撑 TPRM 市场，每一类专注于一个或多个风险领域、行业或客户成熟度级别。Forrester 的新报告《Now Tech：第三方风险管理平台，2022 年第一季度》，根据功能将 22 种主要的 TPRM 技术分为四大类，每一大类都有适合不同类型买家的供应商。

（1）专用技术。这类技术在整个第三方风险管理生命周期当中提供强大功能。它们结合领域专业知识和广泛功能，以支持所有级别的 TPRM 成熟度。

（2）GRC 平台。治理、风险和合规（GRC）平台为众多的风险和合规使用场景提供强大支持。

（3）风险信息交换中心。风险信息交换中心让组织可以访问预先填好和验证的评估结果、多种类型的文档和证据以及分析工具。

（4）专注于垂直领域的供应商。这些提供商拥有扎实的专业技术专长、GRC 平台的广泛功能，并经常提供支持服务，但尤其关注第三方合规要求很复杂的行业。

（来源：安全内参）

4、IDC：2025 年中国网络安全市场规模将超 214 亿美元

IDC 数据显示，2021 年中国网络安全相关支出有望达到 102.6 亿美元。预计到 2025 年，中国网络安全支出规模将达 214.6 亿美元。在 2021-2025 的五年预测期内，中国网络安全相关支出将以 20.5%的年复合增长率增长，增速位列全球第一。

相较于增速放缓的全球网络安全服务市场，**中国安全服务市场将以近全球两倍的五年复合增长率快速增长**。IDC 预测，在 2021-2025 的五年预测期内，中国网络安全服务市场年复合增长率将达到 20.8%，到 2025 年，其市场规模预计将超过 61.1 亿美元。其中，**安全咨询服务（Consulting Services）在未来五年仍为最大的服务子市场**，到 **2025** 年，咨询服务市场的规模将达到 **24.6 亿美元**。与此同时，在安全运营需求不断爆发的大背景下，中国托管安全服务（Managed Security Services）市场发展势头强劲，五年复合增长率预计达到 31.9%。

（来源：安全内参）

5、2022 年全球 IT 行业 10 大预测：网络安全、数字优先成为核心驱动力

IDC 预计，到 2022 年，全球一半以上的经济将基于数字化或受数字化影响，因为大多数产品和服务都将采用数字化交付模式，或者需要数字化增强才能保持竞争力。为了在数字化优先的世界中赢得竞争，组织需要优先投资于数字化工具，以增强物理空间和资产。因此，到 2024 年，一半以上的 ICT 投资将与数字化转型挂钩。

根据 IDC 的最新预测，2022 年中国 ICT 市场（含第三平台与创新加速器技术）规模将达到 7,937 亿美元，比 2021 年增长 9.2%，持续高于 GDP 的增长。**2022 数字化转型支出将达到 3,291 亿美元**，比 2021 年增长 18.6%,数字化转型依然是企业的核心战略。

（来源：安全内参）

6、2022 年中国未来数字化基础架构十大预测

IDC FutureScape 对未来数字化基础架构的预测如下：

（1）敏捷业务战略：到 2023 年，中国 500 强企业将更优先考虑业务目标而非基础设施选择，30%新的工作负载将使用解决方案提供商特定 API 来部署，这些 API 将会增加价值，但同时降低工作负载的可移植性。

（2）供应链完整性：到 2024 年，超过 50%的中国 500 强企业将考虑到业务韧性，将基础设施供应链完整性作为选择厂商的评估标准。

（3）数据安全治理：到 2023 年，随着网络安全隐患的不断增加，大规模数据面临风险，大多数最高层领导者将实施与数据可用性、数据保护和数据治理相关的 KPI，这些 KPI 对企业来说至关重要。

（4）环境、社会和公司治理（ESG）：到 2025 年，鉴于 CIO 依赖基础设施厂商来帮助实现其 ESG 目标，50%中国 500 强企业的数字基础设施方案征询书（RFP）将要求 IT 厂商能用数据来证明企业在 ESG/可持续运营方面的成效。

（5）边缘数据优先：到 2025 年，随着边缘数据的爆炸式增长，超过 50%的中国 500 强企业将把边缘优先数据管理、安全和网络实践嵌入到数据保护计划之中。

（6）工作负载激增：到 2025 年，高依赖性工作负载将激增 5 倍，这将促使 40%的中国 500 强企业使用前后一致的架构治理框架，以此来确保基础设施报告和审计的合规性。

（7）即服务：到 2025 年，50%的中国企业将通过营运开支（opex）预算来为业务线（LOB）和 IT 项目提供经费，并与 KPI 准确对接。

（8）创新基础架构：到 2025 年，60%的中国企业将采用创新计算技术，通过缩短价值生成时间（time to value）来促进业务差异化。

（9）AIOps：到 2026 年，60%的中国 500 强企业将使用 AIOps 解决方案来推动自动化和工作负载分配决策，包括定义成本和绩效指标，以提高韧性和敏捷性。

（10）以应用为中心：到 2026 年，中端市场企业将把 40%的基础设施开支从传统渠道转向更加以应用为中心的技术合作伙伴。

（来源：IDC 中国公众号）

7、零信任安全市场将在 2027 年达到 644 亿美元

据 Research And Markets 数据显示，在 COVID-19 危机中，2020 年全球零信任安全市场估计为 183 亿美元，预计到 2027 年修订后的规模将达到 644 亿美元，复合年增长率为 19.7%。

到 2020 年，美国的零信任安全市场估计为 54 亿美元。作为世界第二大经济体的中国，预计到 2027 年将达到 111 亿美元的市场规模，复合年增长率为 19%。其他值得注意的地区包括日本和加拿大，预计在 2020-2027 年期间分别增长 17.8% 和 17%。在欧洲，预计德国的复合年增长率约为 14.4%。

（来源：helpnetsecurity）

四、勒索事件专题

在认识到数据蕴藏的巨大价值后，越来越多的网络犯罪分子利用勒索软件来牟取非法利益。他们通过加密目标设备上的文件资料来索要赎金以换取解密密钥，甚至窃取企业敏感数据，并威胁在暗网上发布或出售受害者数据，导致企业业务中断或数据泄露，造成严重影响。

本节选取了近期较为典型、活跃的三大勒索软件组织进行分析介绍，旨在为各行各业敲响警钟。

（一）Lapsus$ 勒索组织

数据勒索黑客组织 Lapsus$ 近几月呈现活跃趋势，该组织与常见的勒索软件组织那样加密机密文件不同，Lapsus$ 以大公司的源代码存储库为目标，通过破坏企业系统来窃取源代码、客户列表、数据库和其他有价值的专有数据，然后威胁受害公司若不满足他们的要求则将公开发布其敏感数据。

在过去的几个月里，Lapsus$ 披露了许多针对大型企业的网络攻击，其中针对英伟达（NVIDIA）、三星（Samsung）、沃达丰（Vodafone）、育碧（Ubisoft）和、Impresa、Mercado Libre、微软等的攻击得到了证实。

1、葡萄牙最大的媒体公司 Impresa 遭 Lapsus$勒索攻击

1 月 2 日消息，新年伊始，葡萄牙最大的电视台和报纸媒体 Impresa 就遭到勒索软件攻击而瘫痪，这也是国家级媒体服务首次因

勒索软件攻击而长时间中断。此次攻击背后的勒索软件团伙为Lapsus$。

据悉，受影响的是对 Impresa 运营至关重要的服务器基础设施，该国最主要的广播频道SIC和周报Expresso服务暂时中断。Lapsus$团伙在 Impressa 的所有网站留下勒索赎金要求，并声称已获得对Impresa 的 Amazon Web Services 帐户的访问权限。1 月 2 日，该公司的所有网站处于维护状态，攻击者还利用 Expresso 的 Twitter 帐户发发文称他们仍可访问公司资源。

（来源：GoUpSec）

2、英伟达机密数据、员工信息遭窃，勒索目的直指显卡开源

2 月 23 日，黑客组织 Lapsus$对英伟达进行了网络攻击，并声称窃取了超过 1TB 的数据共计超过 40 万份文件，包括英伟达之后几代显卡的原理图、源代码、英伟达超分辨率技术 DLSS 文件以及英伟达 71335 名员工的电子邮件和密码。Lapsus$还发布了一个 18.9GB 的文件，内含英伟达未发布的 40 系列显卡中的旗舰产品等机密数据。

Lapsus$要求英伟达必须在美国时间 3 月 4 日（北京时间 5 日下午 4 点）结束前开源其用于 macOS、Windows 和 Linux 设备的图形芯片驱动程序，否则将泄露所有数据。此外，Lapsus$宣布将以 100 万美元的价格出售加密 nerf 的 bypass。

据报道，Lapsus$针对英伟达的勒索最初源于该公司对其 RTX 30 系列产品施加的挖矿限制。由于全球缺芯和加密货币大涨，自 2021 年

以来，显卡价格飞速飙升，引起了大量游戏玩家和消费者不满。针对这一情况，英伟达在 2021 年 2 月推出了 LHR，限制了 GeForce RTX 3080、3070 和 3060 Ti 等型号显卡的挖矿能力，以期减少挖矿者抢购显卡的行为。Lapsus$此举目的是让英伟达解除其产品对虚拟货币挖矿功能的限制。

（来源：cnbeta）

3、三星确认遭 Lapsus$ 勒索软件攻击，源代码泄露

3 月 4 日，Lapsus$勒索软件团伙声称从三星电子窃取了大量敏感数据，并泄露了 190GB 的所谓的“三星电子机密源代码”作为黑客攻击的证据。这些文件包括三星 TrustZone 环境中用于敏感操作的源代码、所有生物特征解锁算法、激活服务器的源代码、用于授权和验证三星电子账户的源代码（包括 API 和服务），甚至还有来自高通的机密源代码。Lapsus$将泄露的数据拆分为三个压缩文件，通过点对点网络供外界下载。据外媒报道，已有 400 多人下载这些泄露数据。Lapsus$还声明将部署更多服务器以提升文件下载速度。

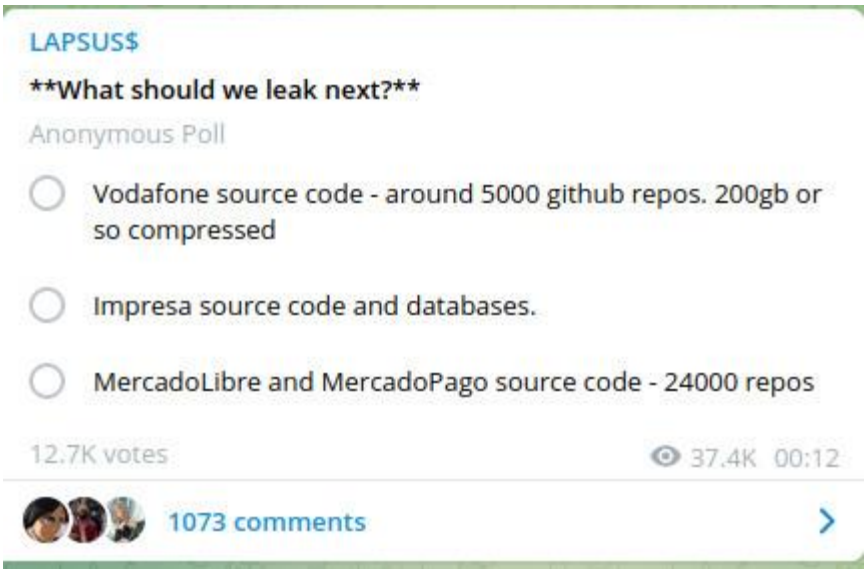
3 月 7 日，三星确认其系统存在数据泄露，并且入侵者可以访问 Galaxy 智能手机中使用的源代码，但此次泄露并不涉及其消费者或员工的个人信息。

（来源：BleepingComputer）

4、黑客组织 Lapsus$发起投票：根据结果公开公司数据

3 月 7 日，在攻破英伟达之后，嚣张的黑客组织 Lapsus$ 在 Telegram 上发出投票帖，通过投票结果来决定接下来公开哪家公司的数据。在投票选项中包括英国电信公司 Vodafone 的源代码、葡萄牙媒体集团 Impresa 的源代码和数据库、南美电子商务公司 MercadoLibre & MercadoPago 的数据库。投票将于 3 月 13 日结束。

（来源：cnbeta）



5、电子商务巨头 Mercado Libre 确认源代码数据泄露

3 月 8 日，阿根廷电子商务巨头 Mercado Libre 确认其部分源代码遭到数据勒索团伙 Lapsus$ 未经授权的访问，并且有大约 300,000 名用户的数据被入侵。

Mercado Libre 表示："根据目前的分析没有发现任何证据表明 IT 基础设施受到了损害。也没有证据表明用户的用户密码、账户余额、投资资金、财务情况或支付卡信息被盗取。目前正在采取严格的措施来防止新的泄露事件发生。"据悉，Mercado Libre 的数据库拥有近 1.4 亿活跃用户，业务遍及阿根廷、巴西、墨西哥、哥伦比亚、智利、委内瑞拉和秘鲁等 18 个国家，是拉丁美洲最大的电子商务和支付生态系统。

（来源：BleepingComputer）

6、沃达丰已开始着手调查 Lapsus$ 所宣称的数据泄露

3 月 11 日，据外媒报道，在 Lapsus$黑客组织声称窃取了其源代码后，沃达丰宣布已展开调查。Lapsus$声称窃取了跨国电信公司沃达丰大约 200 GB 的源代码文件，据称这些文件包含在 5,000 个 GitHub 存储库中。

沃达丰表示，它正在与执法部门合作，调查黑客组织 Lapsus$ 提出的数据泄露指控，还表示勒索中所引用的存储库类型包含的是专有源代码，并不包含客户数据。

（来源：securityaffairs）

7、育碧疑遭 Lapsus$ 黑客组织攻击，造成服务暂时中断

3 月 10 日，育碧疑遭到 Lapsus$黑客组织攻击，该公司称遭遇了一起“网络安全事件”，导致其游戏、系统和服务中断，但目前没有证据表明玩家的个人信息遭泄露。

虽然不能完全确认育碧遭攻击一事与英伟达和三星遭袭事件有相关性，但是，谣言依据主要是源于在黑客组织 Lapsus$运营的 Telegram 主页上，发布了育碧遭网络攻击相关内容的文章链接和一个傻笑的表情符号，从某种角度上看，这种暗示似乎仍认为觉得该组织似乎也对育碧事件负责。不过在育碧官方回应用户的疑问中，并未立即做出回应。

（来源：securityaffairs）

8、微软确认其被 Lapsus$ 勒索组织入侵并窃取了部分源代码

3 月 20 日，Lapsus$ 黑客组织声称其从微软内部 Azure DevOps 服务器窃取了 Bing、Cortana 和其他项目的源代码，并在 Telegram 上发布了所谓的内部源代码存储库的屏幕截图。

3 月 21 日晚上，Lapsus$ 发布了一个 9GB 大小的压缩文件，其中包含他们认为属于微软的 250 多个项目共 37GB 的源代码，包括 90% 的 Bing 源代码以及大约 45%的 Bing Maps 和 Cortana 代码。据安全研究人员称，它们似乎是来自微软的合法内部源代码，这些项目似乎是针对基于 Web 的基础设施、网站或移动应用程序。

3 月 22 日，微软确认其员工的一个账户被 Lapsus$ 入侵，提供了对源代码存储库的有限访问权限。

（来源：BleepingComputer）

9、Okta 确认约有 2.5% 客户受到 Lapsus$ 数据勒索组织攻击影响

3 月 22 日，身份验证服务和身份与访问管理 (IAM) 解决方案提供商 Okta 表示，约有 375 名客户受到 Lapsus$ 数据勒索组织声称的网络攻击的影响。

事件源于数据勒索组织 Lapsus$ 在其 Telegram 频道中发布了据称可以访问 Okta 后端管理控制台和客户数据的屏幕截图。该组织声称已获得对 Okta.com 的“超级用户/管理员”访问权限，并访问了 Okta 的客户数据。

当日晚些时候，Okta 证实，他们在 1 月份遭遇了一起安全事件，当时黑客入侵了其一名支持工程师的笔记本电脑，该笔记本电脑可能会为客户重置密码。“支持工程师确实可以访问屏幕截图中显示的有限数据，例如 Jira 票证和用户列表。支持工程师还可以帮助用户重置密码和重置多因素身份验证（MFA），但无法获取这些密码。”Okta 表示。

（来源：BleepingComputer）

10、Lapsus$ 声称已成功入侵 LG 电子集团

3 月 22 日，数据勒索组织 Lapsus$声称已经成功入侵 LG 电子集团，该组织通过 Telegram 发布了一份文件，声称这是 LG 电子集团员工和服务账户的哈希值。在 8.3MB 的文件中以英文发布了大约 90,000 条姓名，该文件的大小包括总共 88,759 行文本。

“我们认为只有一部分员工的电子邮件地址被泄露，”LG 电子在接受韩国媒体采访时表示，“我们确认了泄露并开始加强安全性。”该公司表示，到目前为止，尚未确认有客户相关信息的泄露。

（来源：pickool）

（二）Conti 勒索软件

Conti 勒索软件家族以 RaaS（勒索软件即服务）形式运营，通过匿名化 Tor 建立赎金支付与数据泄露平台，发布受害者信息及窃取到的数据文件。该组织采用的是新兴的双重勒索策略，即“威胁泄露企业数据+数据加密勒索”，在用勒索软件加密系统之前，会先下载受害者未加密的机密资料，以在受害者拒绝支付赎金以换取解密密钥时，作为进一步的勒索筹码，已有部分案例显示有受害者最终为了保护敏感数据而选择支付赎金。

1、台达电子遭 Conti 勒索软件攻击，或波及苹果和特斯拉

日前，我国台湾地区电子产品制造公司台达电子（Delta Electronics）发布声明称，其受到一起勒索软件攻击，这次攻击发生在 2022 年 1 月 21 日，与 Conti 勒索软件团伙有关。

尽管台达电子方面宣称攻击并未影响其核心生产系统。然而当地媒体报道，有记者已获得一份内部事件报告副本，报告数据显示这次攻击实际情形非常严峻——台达电子 1500 多台服务器和 12000 多台计算机已被攻击者加密。

由于台达电子是目前主流的 UPS 解决方案供应商，并且为苹果和特斯拉等公司供应电源部件。目前尚不清楚此次攻击是否会对其客户的产品供应造成影响。据称，攻击者向这家台湾电子产品制造商索要 1500 万美元的赎金。

（来源：TheRecord）

2、俄乌冲突引发 Conti 网络武器库泄露

俄乌冲突引发民间网络安全能力者的分裂，Conti 勒索软件选择站队俄罗斯，引发一名乌克兰安全研究人员的愤怒，开始疯狂地公开泄露 Conti 内部数据。

据 CyberArk 分析，泄露数据包括 Conti 勒索软件代码、TrickBot 木马代码、Conti 培训材料、Conti/TrickBot 内部交流的各种攻击技巧等，已然是一个小型网络武器库。

这些泄露数据可谓双刃剑，安全研究人员可以了解 Conti 的策略、代码开发、货币化方式、潜在成员身份等信息，采取更可靠的防御手段；恶意软件开发者也可以利用这批数据，指导开发更多类似 TrickBot 的恶意软件。

（来源：secrss）

3、营销巨头 RRD 证实了 Conti 勒索软件攻击中的数据盗窃

1 月 19 日，RR Donnelly 已确认威胁参与者在 12 月的网络攻击中窃取了数据，外媒证实这是一次 Conti 勒索软件攻击。

RR Donnelly (RRD) 是一家领先的综合服务公司，为企业客户提供通信、商业印刷和营销服务。该公司在 200 多个地区拥有 33,000 名员工，2021 年的收入为 49.3 亿美元。

2021 年 12 月 27 日，RRD 曾披露其遭受了“技术环境中的系统入侵”，他们关闭了网络以防止攻击蔓延。2022 年 1 月 15 日，Conti 勒索软件团伙声称对此次攻击负责，并开始泄露据称从 RRD 窃取的 2.5GB 数据。

（来源：BleepingComputer）

4、印尼央行在 Conti 泄露数据后确认勒索软件攻击

1 月 20 日，印度尼西亚共和国中央银行印度尼西亚银行（BI）证实，上个月勒索软件攻击袭击了其网络。印度尼西亚银行发言人表示，

袭击发生后，该银行的运营没有中断。但据 CNN Indonesia 报道，在此次事件中，攻击者窃取了属于印尼银行员工的“非关键数据”。

虽然印度尼西亚银行没有将攻击归咎于特定的勒索软件团伙，但 Conti 在泄露了一些从印度尼西亚银行网络窃取的文件数据后，声称遭到了这次攻击。如果印尼银行不支付赎金，该勒索软件组织声称将有 13.88 GB 的文件泄露。

（来源：BleepingComputer）

（三）LockBit 勒索软件

LockBit 是目前最活跃的勒索软件团伙之一，主要以大公司为目标，索要赎金高达数千万美元，例如 2021 年 8 月埃森哲被索要 5000 万美元（约 3.2 亿人民币）的赎金。

LockBit 同样采用勒索软件即服务形式运营，并升级了勒索策略，以加密和公开敏感数据为主要勒索手段给受害者进一步施压，实现双重勒索。该组织在 2021 年 6 月发布了 LockBit 2.0 新版本，并开始高调招募新的合作伙伴。

1、全球最大轮胎制造商普利司通美洲公司遭 LockBit 勒索攻击，数据被窃取

3 月 11 日消息，LockBit 勒索软件团伙声称对全球最大的轮胎制造商之一普利司通美洲（Bridgestone Americas）公司进行了网络攻击，并窃取了该公司的数据。普利司通在全球拥有数十个生产单位和超过

130,000 名员工，如果公司不支付赎金，Lockbit 计划在 3 月 15 日 23:59 之前泄露被盗数据。

2 月 27 日，普利司通便开始调查当日凌晨发现的“潜在信息安全事件”，而直到 3 月，当 LockBit 勒索软件团伙通过将普利司通美洲公司添加到受害者名单中时，才出现有关该事件的详细信息。目前尚不清楚 LockBit 从普利司通窃取了哪些数据，也不清楚泄露这些数据对该公司有多大的危害。

（来源：BleepingComputer）

2、LockBit 勒索软件组织窃取了包含 10 万名客户信息的 PayBito 数据库

2 月 8 日消息，LockBit 勒索软件团伙声称，他们窃取了加密货币交易所 PayBito 的数据库，该数据库包含全球约 10 万名客户的信息，包括电子邮件地址和“弱”密码哈希值。PayBito 是由全球区块链和 IT 服务公司 HashCash 运营的加密货币交易所，提供比特币、以太币、比特币现金、莱特币和其他几种加密货币的买卖和交易。

目前，部分被盗数据公布在该团伙的 Tor 泄漏网站上。LockBit 勒索软件团伙在其帖子中表示，被盗的数据库包含美国和世界其他国家客户的个人信息。此外，被盗的数据还包括该交易所管理人员的个人数据。该组织声称如果收不到赎金，将在 2022 年 2 月 21 日公布被盗数据。

（来源：Hackread）

《数字安全观察》版块

每周动态/政策解读/行业洞察/技术前瞻/事件分析

策略建议/国际智库精编/信创专刊/数据安全专刊/国防专刊

总编辑：杜跃进

执行编辑：张义荣 韩李云

编委会：360 天枢智库编委会

排版校对：唐会芳

如有反馈 邮件请至 dipperresearch@360.cn